Kongruenciák és Malcev-feltételek

A **T043671** *OTKA-pályázat részletes zárójelentése*

A kutatási terv szerint a pályázat célja az volt, hogy általános algebrákban megvizsgáljuk a kongruenciaháló, a termek, polinomok viselkedése, valamint az algebra szerkezete közötti összefüggéseket, tekintettel az algoritmuselméleti aspektusokra is. Az áttekinthetőség érdekében az eredményeket a következő kategóriákba soroltuk.

1. Kommutátorelmélet, kongruenciaazonosságok, szabad spektrum.
2. A „*Constraint Satisfaction*” probléma.
3. Termekkel kapcsolatos eldönthetőségi problémák.
4. Részben rendezések, hálók.

Az első és negyedik témakör algebrai, a másik kettő az algebra, a kombinatorika és az algoritmuselmélet határterülete. A pályázat résztvevői az alább vázolt eredményekről összesen több mint 50 előadást tartottak nemzetközi fórumokon.

1. Kommutátorelmélet, kongruenciaazonosságok, szabad spektrum.

A moduláris kommutátor egyfajta kapcsolatot létesít az algebrák kongruenciahálója és szerkezete között. A kongruenciaszelídítés elmélete ezt kiterjeszti a nem moduláris esetre is, de csak véges algebrákra működik. E kiterjesztés során természetesen adódik két új fogalom: az *erős* és a *négyszögletes* kommutátor (utóbbit a „kicsi” szabad spektrumok vizsgálata során fedezték föl). Keith Kearnes és Kiss Emil 200 oldalas [26] könyve ezeket, és a hozzájuk tartozó feloldhatóságfogalmat használja föl végtelen algebrák kongruenciahálóinak vizsgálatára, részben általánosítva a véges algebrákra kongruenciaszelídítéssel nyert korábbi eredményeket. A könyv jelenleg lektorálás alatt áll, de letölthető a

`http://spot.colorado.edu/~kearnes/Papers/cong.pdf`

címről. A végtelen algebrák kezelésére új eszközöket kellett kifejleszteni. A lokálisan véges varietások kongruenciaszelídítésben szereplő osztályozását a könyv kiterjeszti minden varietásra. Például ha $\mathcal{V}$ tetszőleges varietás, akkor az alábbiak ekvivalensek:

(1) $\mathcal{V}$-ben teljesül egy nemtriviális kongruenciaazonosság.
(2) $\mathcal{V}$-ben teljesül egy olyan idempotens Malcev-feltétel, ami a félhálók varietásában nem teljesül.
(3) A négyszögletes kommutátor triviális $\mathcal{V}$-ben (bármely két kongruencia kommutátora a metszetük, másképp: a négyszögletes toleranciák mind triviálisak).
(4) D_2 nem részhálója $\mathcal{V}$ egyetlen algebrája kongruenciahálójának sem.

Hasonlóan jellemezhető a kongruenciahálók egyesítés-szemidisztributivitása is, ahol a klasszikus kommutátornak is triviálisnak kell lennie, és az M_3 részhálót is ki kell zárni. Az erős kommutátor trivialitása pedig olyan Malcev-feltételnek felel meg, amely a halmazok varietásában nem teljesülhet. A jellemzésekben olyan konkrét Malcev-feltételek, illetve kongruencia-azonosságok is szerepelnek, amelyek a lokálisan véges esetből már ismerősek. A könyv utolsó fejezetében a szerzők belátják, hogy ha egy varietás reziduálisan kicsi, és teljesít egy nemtriviális kongruencia-azonosságot, akkor moduláris. Bevezetésre kerül a Malcev-féle differenciatermhez hasonló *join-term* fogalma is.

A kongruenciaszelídítés alkalmazásaként a 35 oldalas [25] dolgozat azokat a lokálisan véges varietásokat vizsgálja, ahol a főkongruenciák elsőrendű formulával definiálhatók. Kiderül, hogy a feloldható kongruenciák nilpotensek, az erősen feloldhatók pedig erősen Abel-félék.

Ahogy a „kicsi" szabad spektrum elvezet az erős és a négyszögletes kommutátorhoz, várható, hogy az ennél csak „kicsit" nagyobb szabad spektrumok újabb, természetes és hasznos kommutátorfogalmakat adnak. Ilyen spektrumú algebrákat azonban nehéz találni. Kátai Kamilla, Pluhár Gabriella, Szabó Csaba és Japhet Wood sikerrel járt, a keresett algebrák félcsoportok. A [20] dolgozatban a Brandt-félcsoport szabad spektrumának leírása szerepel. Kötegvarietásokban az n elemmel generált szabad algebra elemszámának logaritmusa

$$\frac{4}{(k-3)!}n^{k-3}\log n - \frac{4}{(k-3)!}n^{k-3}\sum_{j=1}^{k-3}\frac{1}{j} + O(n^{k-4}\log n)\,,$$

ahol k a kötegvarietástól függő állandó.

2. A „Constraint Satisfaction" probléma.

A relációhomomorfizmus-probléma (Constraint Satisfaction Problem, röviden *CSP*) vizsgálata már a nyolcvanas évek óta a számítástudomány egyik fontos iránya. Számos kombinatorikus probléma természetes módon fejezhető ki relációhomomorfizmus-problémaként.

Legyen H egy rögzített, véges relációstruktúra. A $CSP(H)$ eldöntési probléma inputja egy I (azonos típusú) relációstruktúra, a kérdés pedig az, hogy létezik-e $I \to H$ relációhomomorfizmus (azaz olyan leképezés, melynél relációban álló elemek képe mindig a megfelelő relációban áll).

Feder és Vardi érdekes bonyolultságelméleti motivációt találtak a problémakör vizsgálatára. Céljuk olyan, minél nagyobb részosztály keresése *NP*-ben, melyben minden probléma vagy *P*-beli, vagy *NP*-teljes. Ezt a tulajdonságot nevezzük *dichotómiának.* Ha $P \neq NP$, akkor *NP*-ben nincs dichotómia. Feder és Vardi az *NP*-vel ekvivalens *SNP* osztály részosztályait kezdték vizsgálni. Az *SNP* legtermészetesebb részosztálya, mely nem ekvivalens *NP*-vel, és így lehet benne dichotómia, az úgynevezett *MMSNP* (Monotone Monadic Strict *NP*) osztály. Például ilyen nyelvet alkotnak azok az irányítatlan gráfok, melyek csúcshalmaza két részre osztható úgy, hogy egyik rész se tartalmazzon háromszöget, vagy adott (a, b) egész számpárra azok a gráfok, melyeknek van lokális a színezése b színnel.

Feder és Vardi belátták, hogy az *MMSNP* osztály random ekvivalens *CSP*-vel, azaz *CSP* is majdnem ilyen jó jelölt dichotóm osztálynak. Kun Gábor [28]-ban derandomizálja a *CSP* és *MMSNP* közti ekvivalenciát, azaz belátja, hogy a két osztály a szokásos értelemben is ekvivalens. Ehhez bevezeti a hipergráf-expander fogalmát, és hatékonyan konstruál ilyeneket, nagy derékbőséggel. A módszer gráf-expanderekre is új konstrukciókat ad. Ilyen struktúrák konstruálása már gráfok esetében is rendkívül nehéz, így a hipergráfos konstrukció komoly előrelépés az Elméleti Számítástudományban, valamint nagy derékbőségű és kromatikus számú hipergráfok hatékony konstruálását is lehetővé teszi.

A *CSP*, *MMSNP* és *NP* osztályok kapcsolatát elemzi Kun Gábor és Jaroslav Nešetřil a [31], [32], [33] dolgozatokban. Megmutatják, hogy minden *NP*-beli probléma kódolható gráfok injektív, illetve teljes színezett homomorfizmusainak nyelvén, az *MMSNP* nyelvhez rendkívül hasonlóan. Egyszerűen jellemzik azokat az *MMSNP* nyelveket, melyek egyben *CSP* nyelvek is. Ebben egyik fő eszközük a relációstruktúrák (Nešetřil által bevezetett) dualitása: egy véges (F, D) párt duálisnak nevezünk, ha bármely S struktúrának pontosan akkor van homomorfizmusa D-be ha F-nek nincs S-be. Kategóriaelméleti megközelítésük nagyban egyszerűsíti az *MMSNP* és *CSP* osztályok vizsgálatát. Belátják, hogy egy *MMSNP* nyelv megszorítása gráfok egy úgynevezett „korlátos expanziójú” osztályára mindig egyenlő egy *CSP* nyelv megszorításával.

Még kéziratban van Kun Gábor és Claude Tardif eredménye, melyben véletlenszerűen irányított utak dualitásait vizsgálják. Belátják, hogy a duális $1 - o(1)$ valószínűséggel exponenciálisan nagy. Munkájuk érdekes mellékterméke, hogy egy irányított útnak pozitív valószínűséggel nincsen nem identikus endomorfizmusa.

A *CSP* vizsgálatában fontos eseménynek bizonyult az algebrai módszerek bevezetése (Jeavons, Bulatov, Krokhin). Az elmélet kiindulópontja az az észrevétel, hogy $CSP(H)$ bonyolultságát meghatározza az az algebra (klón), melynek alaphalmaza H, műveletei pedig H véges változós, relációtartó, idempotens függvényei. A szokásos algebrai konstrukciók, mint részalgebraképzés, homomorfizmus vagy véges direkt hatványozás a megfelelő algebrákon a *CSP* problémák polinomiális redukcióját indukálják. Így a kiinduló algebra által generált varietás válik a vizsgálódás tárgyává.

Mindez lehetővé teszi a kongruenciaszelídítés módszereinek összekapcsolását a *CSP* problémakörrel. A dichotómiasejtés algebrai formája a következő. Ismeretes, hogy ha az A (véges, idempotens) algebrában szerepel az **1**-es típus, akkor a hozzá tartozó *CSP*-nyelv *NP*-teljes. A sejtés az, hogy ellenkező esetben ez a nyelv *P*-ben van. Ezzel kapcsolatban többféle részeredmény is született. Ha az A algebrának van Malcev-termje, vagy majdnem többségi (near unanimity) termje, akkor a sejtés igaz. A többségi term esetét általánosítva Kiss Emil és Matthew Valeriote a [27] dolgozatban belátják a sejtést akkor, ha az A algebra a $CD(3)$ osztályba tartozik, azaz van három, a kongruenciadisztributivitást biztosító Jónsson-termje.

A sejtésből láthatjuk, hogy minél kevesebb műveletet tartalmaz az A algebra klónja, annál nehezebb a megfelelő *CSP* probléma. Például a teljes gráfhoz tartozó klón csak a projekciókból áll Greenwell és Lovász tétele szerint: a teljes gráf minden hatványának egy homomorfizmusa a teljes gráfba csak egy koordinátától függ. Ezt Kun Gábor és Benoit Larose a [29] cikkben kiterjesztették a teljes gráf minden, a koordináták és a teljes gráf permutációjára invariáns részhalmazára (a triviális kivételektől eltekintve), vagyis az ilyen részgráfok homomorfizmusai a teljes gráfba szintén csak egyetlen koordinátától függenek.

3. Termekkel kapcsolatos eldönthetőségi problémák.

Az *ekvivalencia-probléma* (term equivalence problem), vagy *azonosság-ellenőrzési probléma* (identity checking problem) annak vizsgálata, hogy egy adott algebrában milyen azonosságok teljesülnek, azaz hogy két adott kifejezés (term) megegyezik-e tetszőleges behelyettesítés mellett. A problémát a pályázat kutatói gyűrűkben, félcsoportokban és csoportokban vizsgálták.

A probléma bonyolultsága *gyűrűkre* ismeretes volt: nilpotensekre P-beli, egyébként *coNP*-teljes. Willard és Lawrence a következő kérdést tette fel: mi a nehézsége a problémának, ha csak olyan termeket engedünk meg, amelyek monomok összegei, azaz például $(x+y)^n$ alakú kifejezések nem szerepelhetnek. Ha a gyűrű Jacobson-radikál szerinti faktora kommutatív, a probléma P-ben van. Willard és Lawrence megoldották a problémát olyan véges, egyszerű mátrixgyűrűkre, amelyekben az invertálható elemek nemfeloldható csoportot alkotnak, ilyenkor a probléma *coNP*-teljes.

Szabó Csaba és Vértesi Vera a fennmaradó gyűrűkre belátta, hogy ez a megváltoztatott probléma *coNP*-teljes. A [6] dolgozat szerint a probléma már a kételemű test fölötti 2×2-es mátrixgyűrű multiplikatív félcsoportjában is *coNP*-teljes. A bizonyítás során a szerzők a gráf nem-6-színezhetőség problémáját interpretálják. A [7] dolgozatban a háromelemű test fölötti 2×2-es mátrixgyűrű multiplikatív félcsoportjára látják be ugyanezt, a nem-24-színezhetőséget interpretálva. Az általános eredmény még kéziratban van. A bizonyítás során Zsigmondy tételét és Hilbert 90. tételét felhasználva visszavezetik a problémát a nemfeloldható csoportok feletti problémára, melynek *coNP*-teljessege már ismert (lásd a [24] cikk ismertetését a csoportokról szóló részben).

Félcsoportokra az ekvivalencia-probléma kevésbé tisztázott. A fenti eredmények mellett a [21] és [16] cikkekben Szabó Csaba és Vértesi Vera társszerzőikkel zérusegyszerű félcsoportokban vizsgálták a problémát.

Az ekvivalencia-probléma *csoportelméleti* vonatkozásain a pályázat résztvevői közül Horváth Gábor és Szabó Csaba dolgozott további társszerzőkkel. Korábban is ismert volt, hogy nilpotens csoportokra és bizonyos feloldható csoportokra az ekvivalencia-probléma polinomidőben megoldható. A [24] dolgozatban belátják, hogy minden véges, nem feloldható csoportra az ekvivalenciaprobléma bonyolultsága *coNP*-teljes. A bizonyítás a gráfok k-színezhetőségére való visszavezetéssel történik, ahol k a csoport elemszáma.

A [19] cikkben Horváth Gábor és Szabó Csaba művelettáblával megadott véges csoportokban történő azonosságellenőrzést vizsgálnak bonyolultságelméleti szempontból. Meta-Abel csoportok egy bő osztályára bebizonyítják, hogy egy azonosság ellenőrzése a csoporton belül az azonosság hosszának polinomidejében lehetséges. Ugyanezen csoportokban egyenletek megoldhatóságának bonyolultságát is vizsgálják. Megválaszolják Goldmann és Russel egy 1998-ban feltett kérdését: megmutatják, hogy polinomidőben eldönthető, hogy egy egyenlet megoldható-e a hatelemű S_3 csoport felett.

Ugyancsak termekkel kapcsolatos, bonyolultságelméleti szempontból érdekes kérdés egy véges A algebra által generált varietáshoz való tartozás kérdése egy inputként adott B algebráról. A B algebra pontosan akkor van benne az A által generált varietásban ha az A-ban teljesülő azonosságok B-ben is teljesülnek. Így a probléma nehézségének egy természetes mértéke az úgynevezett β-függvény: adott $n > 0$-hoz $\beta(n)$ a legkisebb olyan k szám, hogy a legfeljebb n elemű B algebrák mindegyikében elegendő a legfeljebb k hosszú azonosságokat ellenőrizni. Kun Gábor és Vértesi Vera a [34] dolgozatban belátja, hogy a β függvény nagyságrendje akármilyen fokú polinomnál nagyobb lehet. A bizonyítás során minden k-hipergráfhoz definiálnak egy-egy algebrát. Egy konstrukcióval visszavezetik a tagsági problémát a hipergráfszínezhetőség problémájára, és belátják, hogy bizonyos kritikus hipergráfokra legalább $O(n^k)$ hosszú azonosságra van szükség. Az alsó becslés úgy adódik, hogy lapos hipergráfalgebrák azonosságaira alkalmas normálformát definiálálnak.

4. Részben rendezések, hálók.

Minden *CSP*-probléma kódolható részbenrendezés retrakciói segítségével, így természetes megközelítés a vizsgálatok megszorítása részbenrendezésekre. Kun Gábor egy még kéziratban lévő dolgozatában kiterjeszti a fundamentális csoport fogalmát részbenrendezésekre, és belátja, hogy minden nemtriviális fundamentális csoportú részbenrendezéshez tartozó retrakcióprobléma *NP*-teljes. Jellemzi ezeket azzal a tulajdonsággal, hogy az általuk generált rendvarietásban nincs korona. Sejtése szerint pontosan ezek az *NP*-teljes retrakcióproblémák. Érdekes topológikus mellékága a kutatásoknak a következő tétel: egy kompakt szimpliciális komplexusnak pontosan akkor retraktuma a zárt körvonal ha fundamentális csoportjának homomorf képe az egész számok additív csoportja.

Kun Gábor és Szabó Csaba az [5] cikkben Jónsson-termeket és majdnem-többségi függvényt konstruálnak polinomidőben (ezekkel rendelkező részbenrendezéseken). Topológikus algoritmusukat használva Larose, Loten és Tardif jellemezték az elsőrendben definiálható *CSP*-problémákat.

Elsősorban részben rendezésekkel kapcsolatos problémákkal foglalkozik Radeleczki Sándor is számos dolgozatában. Stephan Földessel közösen az [1] cikkben részben rendezett halmazok intervallum-fogalmát általánosítja. A [23] dolgozat többek között megmutatja, hogy egy összefüggően részben rendezett véges halmazhoz tartozó rendezés-primál algebra mindig minimális kvázivarietást generál. A [9] és az ezt általánosító [22] cikkben olyan részben-rendezett halmazokról van szó, amelyek minden főfilterén egy rendezésfordító permutáció értelmezhető. Radeleczki és társszerzői megmutatják, hogy ezeknek egy kongruenciadisztributív varietás feleltethető meg. További dolgozataiban kvázirendezések hálóival és pszeudokomplementumok vizsgálatával is foglalkozik.

Hálóelméleti problémákat vizsgál Schmidt Tamás [2] és Fried Ervin [14] dolgozata. Előbbiben Grätzer Györggyel és Robert Quackenbush-sal közösen igazolják, hogy minden véges háló kongruencia-megőrző módon beágyazható egy olyan véges hálóba, melyben minden kongruencia osztályai egymással izomorfak, mint hálók.

Végezetül megemlítjük, hogy Fried Ervin több ismeretterjesztő cikket írt, Kiss Emilnek pedig egy 1000 oldalas tankönyve jelent meg. Ezek a pályázathoz tartozó témákban is végeznek ismeretterjesztő tevékenységet. Prőhle Péternek a kutatásokat segítő algebra program karbantartásában volt fontos szerepe.